



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BB

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,794	12/28/2001	Keichi Teramoto	217811US2RD	3076
22850	7590	09/28/2005		EXAMINER
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314				SCHUBERT, KEVIN R
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 09/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/028,794	TERAMOTO ET AL.
	Examiner Kevin Schubert	Art Unit 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 1 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 28 December 2001.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-18 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) _____ is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) 1-18 are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____.
 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
 5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____.



DETAILED ACTION***Election/Restrictions***

Restriction to one of the following inventions is required under 35 U.S.C. 121:

5 I. Claims 1-2 and 10-11 are drawn to a method for sharing an encrypted data region among two or more processes on a tamper resistant processor, classified in class 713, subclass 194 (Electrical Computers and Digital Processing Systems: Data Processing Protection Using Cryptography: Tamper Resistant).

10 II. Claims 3-7 and 12-16 are drawn to a method for specific key management processing in order to accomplish sharing an encrypted data region among two or more processes on a tamper resistant processor, classified in class 380, subclass 277 (Cryptography: Key Management). The key management is accomplished in part by operating each process among the two processes to generate a hidden data region of the each process (part b), operating the two processes to generate a mutually different key pairs to be used and carrying out the key exchange between the two processes (part c), and operating the each process to generate a common key according to the key exchange (part d).

15 III. Claims 8-9 and 17-18 are drawn to a method for sharing an encrypted data region among three or more processes on a tamper resistant processor, classified in class 713, subclass 194 (Electrical Computers and Digital Processing Systems: Data Processing Protection Using Cryptography: Tamper Resistant).

20

The inventions are distinct each from each other because:

25 Inventions I,II, and III are related as subcombinations disclosed as usable together in a single combination.

 Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct each from each other if they are shown to be separately usable. In the instant case invention II has separate utility because it incorporates

Art Unit: 2137

a specific key exchange protocol whereby the two processes generate mutually different key pairs to be used in a key exchange (part c) and the two processes generate a common key according to the key exchange (part d). Additionally, the common key and data used in a course of the key exchange is stored in a hidden data region of each process (part f). See MPEP 806.05(d).

5 Inventions I and III are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct each from each other if they are shown to be separately usable. In the instant case, invention I has separate utility from invention III such as being used as method for sharing an encrypted data region among two or more processes. 10 Additionally, invention I does not require the particulars of the specific key exchange protocol disclosed in invention III. See MPEP 806.05(d).

15 Inventions II and III are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct each from each other if they are shown to be separately usable. In the instant case, invention II has separate utility from invention III such as being used as a method for sharing an encrypted data region among two or more processes. Additionally, invention II does not require particulars presented in invention III such as using the encrypted key notification region to notify the common key to each client process. See MPEP 806.05(d).

20 Because these inventions are distinct for the reasons given and have acquired separate classification in two distinct classes, restriction for examination purposes is proper. The examiner further notes the present burden in examining invention III which requires a search for sharing an encrypted data region among three or more processes in contrast to inventions I and II and which also requires searching separate key distribution subclasses (such as 380/278 Cryptography: Key Distribution) for the limitation of an encrypted key notification region used to notify the common key to each client process. A complete response to this requirement must include an election of 25 the invention to be examined even if the requirement is traversed.

Art Unit: 2137

Conclusion

A shortened statutory period for response is set to expire one month (not less than 30 days) from the mail date of this letter. Failure to respond within the period for response will result in ABANDONMENT of the application (see 35 U.S.C. 133, M.P.E.P. 710.02, 710.02(b)).

5 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3868. The fax phone number for the organization where 10 this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should 15 you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS

20


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER